STRATA

Secure hybrid access

Unifying cloud and on-premises worlds

Strata's Maverics Identity Orchestrator™ provides a Zero Trust approach to enabling access to on-premises apps from the cloud. Maverics extends standards-based authentication from cloud identity systems to on-premises apps, providing sophisticated last-mile integration with no app rewrites.

Our identity orchestration enables incremental moves to the cloud while supporting the coexistence between old and new identity systems. Consistency between cloud and on-premises identity systems means identity and policies that work seamlessly across both.

Challenges with secure hybrid access

Many apps built before the cloud's Zero Trust architecture were not designed to work across hostile networks.

- Legacy IAM software was not designed to work in cloud environments and must be replaced with cloud-native identity.
- Interoperability between new cloud identity systems and existing on-premises identity systems is required.
- Most existing network configurations are not granular enough to control access (identity context data).
- Granular access policies are needed to support Zero Trust's identity as the new perimeter model.
- Moving apps to the cloud and upgrading identity systems means expensive and time-consuming rewrites and maintenance of custom code.

Benefits of secure hybrid access

Any portal. All your cloud and legacy apps

Maverics enables the delivery of on-premises apps through cloud portals from Azure AD or Okta. Easily extend SSO sessions from the cloud to on-premises apps and deliver them to your users through a convenient portal or your app.

Maverics can also be used to mix and match apps and IDPs for different users, based on what works best for your use case. Maverics doesn't lock you into any single portal but instead delivers a wide variety of apps including Citrix-hosted, SaaS, and more. Maverics assembles the solution that is right for the app, the platform, and the users accessing it.

Effortless SAML/OIDC enablement. No rewrites required.

Maverics transforms SAML/OIDC sessions into HTTP headers with smart mapping capabilities; meaning no rewriting or touching existing apps. Maverics even supports sessions for many legacy Web apps that must move to the cloud, without compromising security or usability.

Zero trust with zero limits

Maverics can assemble authentication, MFA, device verification, granular authorization, and risk scoring based on the needs of applications and the sensitivity of your data. Build intelligent identity flows and swap in the services needed as your needs or the threat landscape changes.

Incremental migrations. Breakthrough flexibility.

Maverics enables gradual lift and shift of different apps to the cloud and selective migration of identity systems. Maverics gateways and proxies play nicely with existing network topologies enabling legacy SiteMinder, OAM, ClearTrust, Ping, and Active Directory to coexist seamlessly with cloud identity from Azure AD and Okta.

Unify identity across clouds and on-premises environments

Maverics' Identity Control Plane enables changes in identities on cloud systems like Azure AD and Okta to be propagated back on-premises to keep identity consistent across new and old identity systems.

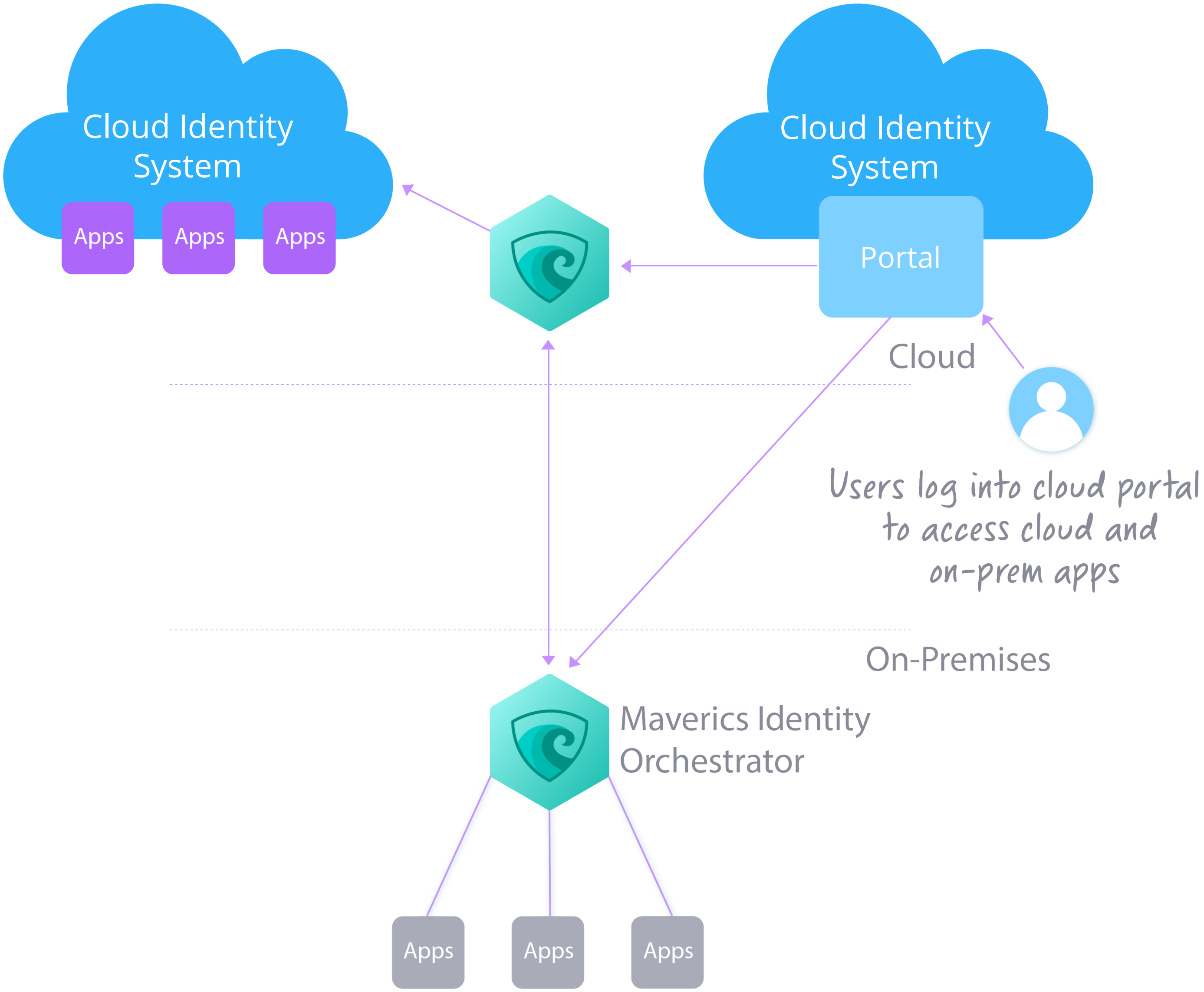
Business impact

- Make on-premises apps available quickly to remote workers without the complexity or expense of additional VPNs.
- Improve predictability and flexibility through incremental migrations versus the risk of Big Bang switches.
- Save money and time by avoiding rewriting apps to make them work on the cloud or with new identity systems
- Preserve the user experience with no changes.
- Gradually deprovision expensive and bloated legacy identity infrastructure and save on support costs.

How maverics secure hybrid access works

- Deployed on-premises and in your cloud platforms as a simple, lightweight service.
- Runs as either a standalone cloud proxy or integrated directly into web and app servers through a unique gateway model.
- Defines and registers on-premises apps to Azure AD or Okta and to Maverics.
- Accepts authentication from trusted identity systems like Azure AD and Okta and then passes sessions to apps using the appropriate session technology.
- Assemble consistent identity profiles from any number of identity and attribute providers and then pass this identity context into apps as part of the last mile integration process.

How secure hybrid access works


Cloud Identity System
Apps
Apps
Apps
Cloud Identity System
Portal
Cloud
Users log into cloud portal to access cloud and on-prem apps
On-Premises
Maverics Identity Orchestrator
Apps
Apps
Apps